PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2000-101984**

(43)Date of publication of application : **07.04.2000**

(51)Int.CI. **H04N 7/167**
H04H 1/02
H04L 9/08
H04N 7/16

(21)Application number : **10-270113**

(22)Date of filing : **24.09.1998**

(71)Applicant : **HITACHI LTD**

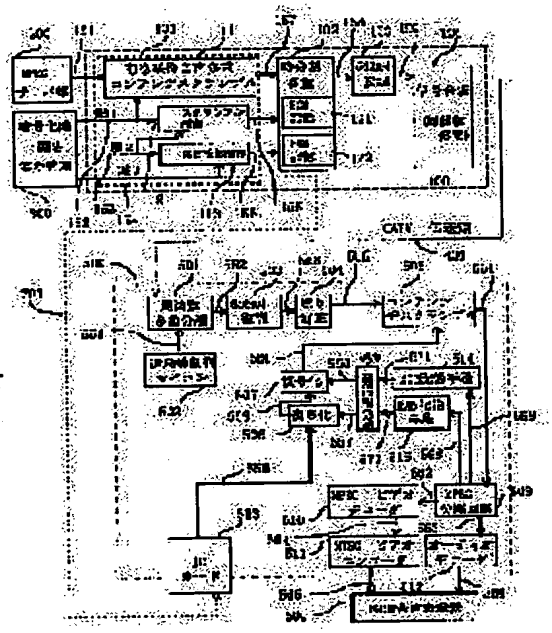
(72)Inventor : **TANAKA HIROMI**
NODA TSUTOMU
NISHIDA MASAMI

(54) LIMITED RECEIVING SYSTEM OF CABLE TELEVISION, AND ITS TRANSMITTER AND ITS RECEIVER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a transmitter-receiver whose program selection channel time is short in a limited receiving system for digital cable television.

SOLUTION: A transmitter side is provided with a multiplexer, which has digital data in a transport stream format and a function that performs time division multiplexing of ECM information and EMM information, also stores the ECM information and the EMM information and repeatedly transmits them. Receivers 500 and 600 sides are provided with an ECM storing means 514 and an EMM storing means 515 for storing the ECM information and the EMM information for every corresponding contracted channel. Scramble is released by using the information stored in these means 514 and 515, until the ECM information and the EMM information are updated.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－101984
（P2000－101984A）
(43)公開日　平成12年４月７日(2000.4.7)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｎ　7/167		Ｈ０４Ｎ　7/167	Ｚ	５Ｃ０６４
Ｈ０４Ｈ　1/02		Ｈ０４Ｈ　1/02	Ｆ	５Ｊ１０４
Ｈ０４Ｌ　9/08		Ｈ０４Ｎ　7/16	Ｃ	
Ｈ０４Ｎ　7/16		Ｈ０４Ｌ　9/00	６０１Ａ	
			６０１Ｂ	

審査請求　未請求　請求項の数24　ＯＬ　（全 20 頁）　最終頁に続く

(21)出願番号　特願平10－270113

(22)出願日　平成10年９月24日(1998.9.24)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　田中　大幹
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所ＡＶ事業部内

(72)発明者　野田　勉
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所マルチメディアシステム開発本部内

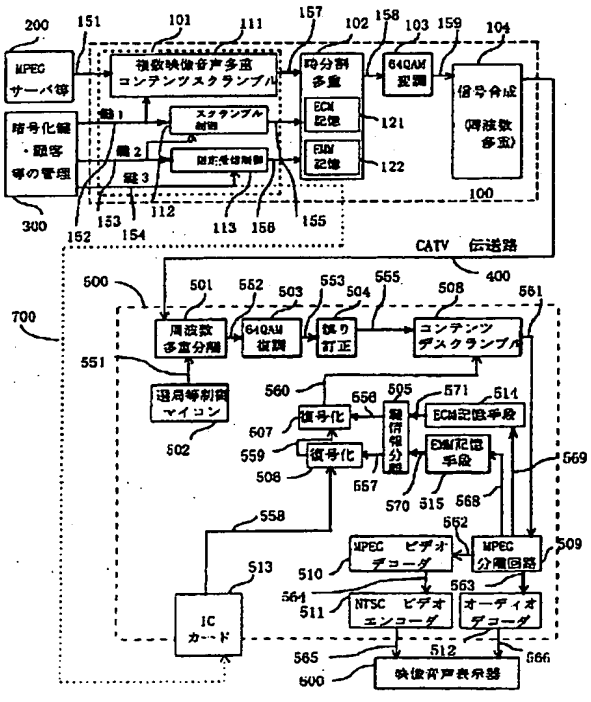
(74)代理人　100061893
弁理士　高橋　明夫　（外１名）

最終頁に続く

(54)【発明の名称】　ケーブルテレビの限定受信システム並びその送信装置及びその受信装置

(57)【要約】
【課題】デジタルケーブルテレビの限定受信システムにおいて、番組選局時間の短い送受信装置を提供することにある。
【解決手段】送信装置側ではトランスポートストリーム形式のデジタルデータとＥＣＭ情報やＥＭＭ情報を時分割多重すると共にＥＣＭ情報およびＥＭＭ情報を記憶して繰り返し送出する機能を有する多重化装置を備え、受信装置側では対応する契約チャンネル毎にＥＣＭ情報及びＥＭＭ情報ををを記憶するＥＣＭ記憶手段とＥＭＭ記憶手段とを備え、ＥＣＭ情報およびＥＭＭ情報が更新されるまではこのＥＣＭ記憶手段及びＥＭＭ記憶手段に記憶された情報を用いてスクランブルを解除する。

図１



1

【特許請求の範囲】

【請求項１】第１の鍵データを第２の鍵データによって暗号化する手段、第２の鍵データを第３の鍵データによって暗号化する手段、前記暗号化された第１の鍵データによって送信するコンテンツデータをスクランブルする手段、前記スクランブル手段から取り出されたトランスポートストリーム形式の前記コンテンツデータ、暗号化された前記第１の鍵データを含むＥＣＭ情報及び暗号化された前記第２の鍵データを含むＥＭＭ情報を時分割多重する手段、前記時分割多重手段に設けられた前記ＥＣＭ情報を繰り返し出力するためのＥＣＭ記憶手段、前記時分割多重手段の出力を変調する手段を備えた送信装置と、

前記デジタル変調されたコンテンツデータ、前記ＥＣＭ情報、前記ＥＭＭ情報を復調する手段、第３の鍵データの出力手段、前記ＥＣＭ情報及び復号された前記第１の鍵データのいずれか一方を記憶する第１の記憶手段、前記ＥＭＭ情報及び復号された前記第２の鍵データのいずれか一方を記憶する第２の記憶手段、暗号化された前記第２の鍵データを前記第３の鍵データを用いて復号する第２の鍵データ復号手段、暗号化された前記第１の鍵データを前記復号された第２の鍵データを用いて復号する第１の鍵データ復号手段、復号された前記第１の鍵データを用いて前記コンテンツデータのスクランブルを解除する手段を備え、前記第１、前記第２の記憶手段の出力を用いてスクランブルを解除する受信装置と、

から構成されることを特徴とするケーブルテレビの限定受信システム。

【請求項２】請求項１記載のケーブルテレビの限定受信システムにおいて、前記送信装置の前記時分割多重手段にＥＭＭ情報を繰り返し出力するためのＥＭＭ記憶手段を設けることを特徴とするケーブルテレビの限定受信システム。

【請求項３】請求項１記載のケーブルテレビの限定受信システムにおいて、前記受信装置の前記第１の記憶手段はＥＣＭ情報を記憶し、前記第２の記憶手段はＥＭＭ情報を記憶することを特徴とするケーブルテレビの限定受信システム。

【請求項４】請求項１記載のケーブルテレビの限定受信システムにおいて、前記受信装置の前記第１の記憶手段は復号された第１の鍵データを記憶し、前記第２の記憶手段は復号された第２の鍵データを記憶することを特徴とするケーブルテレビの限定受信システム。

【請求項５】請求項１記載のケーブルテレビの限定受信システムにおいて、前記受信装置の前記第１の記憶手段にはＥＣＭ情報を記憶し、前記第２の記憶手段には復号された第２の鍵データを記憶することを特徴とするケーブルテレビの限定受信システム。

【請求項６】第１の鍵データを第２の鍵データによって暗号化する手段と、第２の鍵データを第３の鍵データによって暗号化する手段と、暗号化された前記第１の鍵データによって送信するコンテンツデータをスクランブルする手段と、前記スクランブル手段から取り出されたトランスポートストリーム形式の前記コンテンツデータ、暗号化された前記第１の鍵データを含むＥＣＭ情報及び暗号化された前記第２の鍵データを含むＥＭＭ情報を時分割多重する手段と、前記時分割多重手段に設けられ、前記ＥＣＭ情報を繰り返し出力するためのＥＣＭ記憶手段と、前記時分割多重手段の出力を変調して送信する手段とを備えることを特徴とするケーブルテレビの送信装置。

【請求項７】請求項６記載の送信装置において、前記送信装置の前記時分割多重手段に前記ＥＭＭ情報を繰り返し出力するためのＥＭＭ記憶手段を設けることを特徴とするケーブルテレビの送信装置。

【請求項８】送信装置から送付されたスクランブルされたコンテンツデータ、ＥＣＭ情報、ＥＭＭ情報からコンテンツデータのスクランブルを解除するために、第３の鍵データの出力手段と、前記ＥＣＭ情報及び復号された前記第１の鍵データのいずれか一方を記憶する第１の記憶手段と、前記ＥＭＭ情報及び復号された前記第２の鍵データのいずれか一方を記憶する第２の記憶手段と、暗号化された前記第２の鍵データを前記第３の鍵データを用いて復号する第２の鍵データ復号手段と、暗号化された前記第１の鍵データを前記復号された第２の鍵データを用いて復号する第１の鍵データ復号手段と、復号された前記第１の鍵データを用いて前記コンテンツデータのスクランブルを解除する手段を備え、前記第１、前記第２の記憶手段の出力を用いてスクランブルを解除することを特徴とするケーブルテレビの受信装置。

【請求項９】請求項８記載のケーブルテレビの限定受信システムにおいて、前記受信装置の前記第１の記憶手段は前記ＥＣＭ情報を記憶し、前記第２の記憶手段は前記ＥＭＭ情報を記憶することを特徴とするケーブルテレビの受信装置。

【請求項１０】請求項８記載のケーブルテレビの受信装置において、前記受信装置の前記第１の記憶手段は復号された第１の鍵データを記憶し、前記第２の記憶手段は復号された第２の鍵データを記憶することを特徴とするケーブルテレビの受信装置。

【請求項１１】請求項８記載のケーブルテレビの受信装置において、前記受信装置の前記第１の記憶手段はＥＣＭ情報を記憶し、前記第２の記憶手段は復号された第２の鍵データを記憶することを特徴とするケーブルテレビの受信装置。

【請求項１２】請求項８記載のケーブルテレビの受信装置において、前記第１の記憶手段の出力を用いて前記スクランブル解除手段でコンテンツデータのスクランブルが解除されない場合には、送信されてきたＥＣＭ情報を用いて前記第１の記憶手段を更新し、前記第１の記憶手

段の出力を用いてコンテンツデータのスクランブルを解除することを特徴とするケーブルテレビの受信装置。

【請求項１３】請求項８記載のケーブルテレビの受信装置において、前記第２の記憶手段の出力を用いて前記第１の鍵データの復号ができない場合には、送信されてきたＥＭＭ情報で前記第２の記憶手段を更新し、前記更新された第２の記憶手段の出力を用いて前記第１の鍵データを復号することを特徴とするケーブルテレビの受信装置。

【請求項１４】トランスポートストリーム形式のデジタルデータを暗号化して伝送するケーブルテレビシステムにおいて、

映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段、

受信側でコンテンツのスクランブルを解除するために必要となる第１の鍵データの暗号化されたデータを含むＥＣＭ情報を生成しスクランブル装置を制御するスクランブル制御装置、

前記第１の鍵データの暗号化を解除する場合に必要となる第２の鍵データを含むＥＭＭ情報を生成する限定受信制御装置、

第２の鍵データの暗号化を解除するために必要となる第３の鍵データ及び前記第１、前記第２の鍵データ及び顧客情報を管理する鍵情報管理装置、

トランスポートストリーム形式のデジタルデータと前記ＥＣＭ情報や前記ＥＭＭ情報を時分割多重すると共に前記ＥＣＭ情報及び前記ＥＭＭ情報を記憶して繰り返し送出する機能を有する多重化装置、

前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段、

複数の被変調波を周波数多重して伝送路に送出する信号合成手段、

を備えた送信装置と、

周波数多重されて伝送されたデジタル被変調波を復調する復調手段、前記復調手段で得られた前記ＥＣＭ情報より前記第１の鍵データを復号する第１の鍵データ復号手段、

前記復調手段で得られた前記ＥＭＭ情報より前記第２の鍵データを復号する第２の鍵データ復号手段、

前記ＥＣＭ情報を対応する契約チャンネル毎に記憶するＥＣＭ記憶手段、

前記ＥＭＭ情報を対応する契約チャンネル毎に記憶するＥＭＭ記憶手段、

前記復調手段で得られたコンテンツスクランブルのかかった前記データから前記第１の鍵データ復号手段で得られた第１の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段、

を備えた受信装置と、

から構成され、ＥＣＭ情報に変更があるまでは契約チャンネルを選局する毎に前記ＥＣＭ記憶手段に記憶したＥＣＭ情報を利用して、このデータを一旦前記第１の鍵データ復号手段において復号することにより前記第１の鍵データを抽出し、この抽出した前記第１の鍵データを用いて前記復調手段で得られたコンテンツスクランブルのかかった前記データより前記デスクランブル手段によって前記トランスポートストリーム形式のデジタルデータを得ることを特徴とするケーブルテレビの限定受信システム。

【請求項１５】トランスポートストリーム形式のデジタルデータを暗号化して伝送するケーブルテレビシステムにおいて、

映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段、

受信側でコンテンツのスクランブルを解除するために必要となる第１の鍵データの暗号化されたデータを含むＥＣＭ情報を生成しスクランブル装置を制御するスクランブル制御装置、

前記第１の鍵データの暗号化を解除する場合に必要となる第２の鍵データを含むＥＭＭ情報を生成し多重化装置へ出力する限定受信制御装置、

前記第２の鍵データの暗号化を解除するために必要となる第３の鍵データ、前記第１、前記第２の鍵データ及び顧客情報を管理する鍵情報管理装置、

トランスポートストリーム形式のデジタルデータと前記ＥＣＭ情報や前記ＥＭＭ情報を時分割多重すると共に前記ＥＣＭ情報及び前記ＥＭＭ情報を記憶して繰り返し送出する機能を有する多重化装置、

前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段、

複数の被変調波を周波数多重して伝送路に送出する信号合成手段、とを備えた送信装置と、

周波数多重されて伝送されたデジタル被変調波を復調する復調手段と、前記復調手段で得られた前記ＥＣＭ情報より前記第１の鍵データを復号する第１の鍵データ復号手段、

前記復調手段で得られた前記ＥＭＭ情報より前記第２の鍵データを復号する第２の鍵データ復号手段、

前記第１の鍵データ復号手段によって復号された前記第１の鍵データ自体を対応する契約チャンネル毎に記憶する第１の鍵データ記憶手段、

前記第２の鍵データ復号手段によって復号された前記第２の鍵データ自体を対応する契約チャンネル毎に記憶する第２の鍵データ記憶手段、

前記復調手段で得られたコンテンツスクランブルのかかったデータから前記ＥＣＭ復号手段から得られた復号化された前記第１の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段、

とを備えた受信装置と、

から構成され、前記ＥＣＭ情報または前記ＥＭＭ情報に

変更があるまでは前記鍵データ記憶手段に記憶された鍵データを利用して前記デスクランブル手段によって前記復調手段で得られたコンテンツスクランブルのかかったデータからトランスポートストリーム形式のデジタルデータを得ることを特徴とするケーブルテレビの限定受信システム。

【請求項１６】暗号化されたトランスポートストリーム形式のデジタルデータを送信するために、映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段と、受信側でコンテンツのスクランブルを解除するために必要となる第１の鍵データの暗号化されたデータを含むＥＣＭ情報を生成しスクランブル装置を制御するスクランブル制御装置と、前記第１の鍵データの暗号化を解除する場合に必要となる第２の鍵データを含むＥＭＭ情報を生成し多重化装置へ出力する限定受信制御装置と、前記第２の鍵データの暗号化を解除するために必要となる第３の鍵データ、前記第１、前記第２の鍵データ及び顧客情報を管理する鍵情報管理装置と、トランスポートストリーム形式のデジタルデータと前記ＥＣＭ情報や前記ＥＭＭ情報を時分割多重すると共に前記ＥＣＭ情報及び前記ＥＭＭ情報を記憶して繰り返し送出する機能を有する多重化装置と、前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段と、複数の被変調波を周波数多重して伝送路に送出する信号合成手段とを備えることを特徴とするケーブルテレビの送信装置。

【請求項１７】周波数多重されて伝送されたデジタル被変調波を復調する復調手段と、前記復調手段で得られたＥＣＭ情報より第１の鍵データを復号する第１の鍵データ復号手段と、前記復調手段で得られたＥＭＭ情報より第２の鍵データを復号する第２の鍵データ復号手段と、前記ＥＣＭ情報を対応する契約チャンネル毎に記憶するＥＣＭ記憶手段と、前記ＥＭＭ情報を記憶するＥＭＭ記憶手段と、前記復調手段で得られたコンテンツスクランブルのかかったデータから前記第１の鍵データ復号手段で得られた第１の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段とを備えることを特徴とするケーブルテレビの受信装置。

【請求項１８】請求項１７記載のケーブルテレビの受信装置において、前記受信装置が映像や音声の選択をするためのいわゆる選局動作をする場合、まず前記ＥＣＭ記憶手段に記憶されたＥＣＭ情報を用いて前記第１の鍵データを復号して前記デスクランブル手段に供給し、前記第１の鍵データでデスクランブル処理がされない場合には前記復調手段から新しくＥＣＭ情報を抽出して前記ＥＣＭ記憶手段に記憶されたＥＣＭ情報を更新し、更新されたＥＣＭ情報によって第１の鍵データを復号して前記デスクランブル手段に供給してスクランブル解除することを特徴とするケーブルテレビの受信装置。

【請求項１９】周波数多重されて伝送されたデジタル被変調波を復調する復調手段と、前記復調手段で得られたＥＣＭ情報より第１の鍵データを復号する第１の鍵データ復号手段と、前記復調手段で得られたＥＭＭ情報より第２の鍵データを復号する第２の鍵データ復号手段と、前記第１の鍵データ復号手段によって復号された前記第１の鍵データ自体を対応する契約チャンネル毎に記憶する第１の鍵データ記憶手段と、前記第２の鍵データ復号手段によって復号された前記第２の鍵データ自体を対応する契約チャンネル毎に記憶する第２の鍵データ記憶手段と、前記復調手段で得られたコンテンツスクランブルのかかったデータから前記ＥＣＭ復号手段で得られた鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段とを備えたことを特徴とするケーブルテレビの受信装置。

【請求項２０】請求項１９記載のケーブルテレビの受信装置において、前記受信装置が映像や音声の選択をするためのいわゆる選局動作をする場合、まず前記第１の鍵データ記憶手段に記憶された前記第１の鍵データを前記デスクランブル手段に用い、デスクランブル処理がされない場合には前記復調手段から新しくＥＣＭ情報を抽出して前記第１の鍵データ復号手段によって第１の鍵データを復号して前記第１の鍵データ記憶手段に記憶された第１の鍵データを更新し、前記更新された第１の鍵データを前記デスクランブル手段に供給してスクランブルを解除することを特徴とするケーブルテレビの受信装置。

【請求項２１】トランスポートストリーム形式のデジタルデータを暗号化して伝送するケーブルテレビシステムにおいて、

映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段、受信側でコンテンツのスクランブルを解除するために必要となる第１の鍵データの暗号化されたデータを含むＥＣＭ情報を生成しスクランブル装置を制御するスクランブル制御装置、

前記第１の鍵データの暗号化を解除する場合に必要となる第２の鍵データを含むＥＭＭ情報を生成し多重化装置へ出力する限定受信制御装置、

前記第２の鍵データの暗号化を解除するために必要となる第３の鍵データ、前記第１、前記第２の鍵データ及び顧客情報を管理する鍵情報管理装置、

トランスポートストリーム形式のデジタルデータと前記ＥＣＭ情報や前記ＥＭＭ情報を時分割多重すると共に前記ＥＣＭ情報を記憶して繰り返し送出する機能を有する多重化装置、

前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段、

複数の被変調波を周波数多重して伝送路に送出する信号合成手段、

とを備えた送信装置と、

周波数多重されて伝送されたデジタル被変調波を復調する復調手段、前記復調手段で得られた前記ＥＣＭ情報より前記第１の鍵データを復号する第１の鍵データ復号手段、
前記復調手段で得られた前記ＥＭＭ情報より前記第２の鍵データを復号する第２の鍵データ復号手段、
前記ＥＣＭ情報を対応する契約チャンネル毎に記憶するＥＣＭ記憶手段、
前記ＥＭＭ情報を対応する契約チャンネル毎に記憶するＥＭＭ記憶手段、
前記復調手段で得られたコンテンツスクランブルのかかったデータから前記第１の鍵データ復号手段で得られた前記第１の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段、
とを備えた受信装置と、
から構成され、前記ＥＣＭ情報に変更があるまでは契約チャンネルを選局する毎に前記ＥＣＭ記憶手段に記憶した前記ＥＣＭ情報を利用するために、このデータを一旦前記第１の鍵データ復号手段で復号して前記第１の鍵データを抽出し、この抽出された前記第１の鍵データを用いて前記復調手段で得られたコンテンツスクランブルのかかったデータより前記デスクランブル手段によってトランスポートストリーム形式のデジタルデータを得ることを特徴とするケーブルテレビの限定受信システム。

【請求項２２】トランスポートストリーム形式のデジタルデータを暗号化して伝送するケーブルテレビシステムにおいて、
映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段、
受信側でコンテンツのスクランブルを解除するために必要となる第１の鍵データの暗号化されたデータを含むＥＣＭ情報を生成しスクランブル装置を制御するスクランブル制御装置、
前記第１の鍵データの暗号化を解除する場合に必要となる第２の鍵データを含むＥＭＭ情報を生成し多重化装置へ出力する限定受信制御装置、
前記第２の鍵データの暗号化を解除するために必要となる第３の鍵データ、前記第１、前記第２の鍵データ及び顧客情報を管理する鍵情報管理装置、トランスポートストリーム形式のデジタルデータと前記ＥＣＭ情報や前記ＥＭ
Ｍ情報を時分割多重すると共に前記ＥＣＭ情報を記憶して繰り返し送出する機能を有する多重化装置、
前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段、
複数の被変調波を周波数多重して伝送路に送出する信号合成手段、
とを備えた送信装置と、
周波数多重されて伝送されたデジタル被変調波を復調する復調手段、
前記復調手段で得られた前記ＥＣＭ情報より前記第１の鍵データを復号する第１の鍵データ復号手段、
前記復調手段で得られた前記ＥＭＭ情報より前記第２の鍵データを復号する第２の鍵データ復号手段、
前記ＥＣＭ情報を対応する契約チャンネル毎に記憶するＥＣＭ記憶手段、
前記第２の鍵データ復号手段によって復号された前記第２の鍵データ自体を対応する契約チャンネル毎に記憶する第２の鍵データ記憶手段、
前記復調手段で得られたコンテンツスクランブルのかかったデータから前記第１の鍵データ復号手段で得られた前記第１の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段、
とを備えた受信装置と、
から構成され、前記ＥＣＭ情報に変更があるまでは契約チャンネルを選局する毎に前記ＥＣＭ記憶手段に記憶した前記ＥＣＭ情報を利用すると共に、前記ＥＭＭ情報に変更があるまでは前記鍵データ記憶手段に記憶された鍵データを利用するために、このデータを一旦前記第１の鍵データ復号手段で復号して前記第１の鍵データを抽出し、この抽出された前記第１の鍵データを用いて前記復調手段で得られたコンテンツスクランブルのかかったデータより前記デスクランブル手段によってトランスポートストリーム形式のデジタルデータを得ることを特徴とするケーブルテレビの限定受信システム。

【請求項２３】周波数多重されて伝送されたデジタル被変調波を復調する復調手段と、前記復調手段で得られたＥＣＭ情報より第１の鍵データを復号する第１の鍵データ復号手段と、前記復調手段で得られたＥＭＭ情報より第２の鍵データを復号する第２の鍵データ復号手段と、前記ＥＣＭ情報を対応する契約チャンネル毎に記憶するＥＣＭ記憶手段と、前記第２の鍵データ復号手段によって復号された前記第２の鍵データ自体を対応する契約チャンネル毎に記憶する第２の鍵データ記憶手段と、前記復調手段で得られたコンテンツスクランブルのかかったデータから前記第１の鍵データ復号手段で得られた第１の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段とを備えることを特徴とするたケーブルテレビの受信装置。

【請求項２４】請求項２３記載のケーブルテレビの受信装置において、前記受信装置が映像や音声の選択をするためのいわゆる選局動作をする場合、まず前記ＥＣＭ記憶手段に記憶されたＥＣＭ情報を用いて前記第１の鍵データを復号して前記デスクランブル手段に用い、デスクランブル処理がされない場合には前記復調手段から新しくＥＣＭ情報を抽出して前記ＥＣＭ記憶手段に記憶された前記ＥＣＭ情報を更新し、その更新されたＥＣＭ情報によって第１の鍵データを復号して前記デスクランブル手段に供給してスクランブル解除をすることを特徴とするケーブルテレビの受信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、テレビジョン放送の受信者を特定して受信を許可する限定受信方式に関わり，特にＣＡＴＶ（Ｃａｂｌｅ Ｔｅｌｅｖｉｓｉｏｎ）伝送路などを使用したデジタル有線テレビジョン放送の限定受信システム並びにその送信装置及びその受信装置に関するものである。

【０００２】

【従来の技術】従来、ケーブルテレビと呼ばれるＣＡＴＶ伝送路を使用したテレビジョン放送における限定受信方式については、コロナ社発行、（社）電子機械工業会ケーブルテレビ技術委員会編「ケーブルテレビ技術入門」に記述されている。その記述によれば、１ＷＡＹアドレッサブルシステムと呼ばれる方式が記述されている。この方式は、受信側ホームターミナル内のデスクランブル機能を送信側からのＦＳＫ（Ｆｒｅｑｕｅｎｃｙ Ｓｈｉｆｔ Ｋｅｙｉｎｇ）変調の下り回線で制御している。そのスクランブルシステムの詳細な記述はないが、以下の経緯で限定受信方式が進歩しながら変わってきている。まず、簡単な限定受信方式として、映像信号を伝送しているチャンネル以外の帯域でＦＳＫ変調などで伝送される下り回線の制御情報によってＣＡＴＶ受信機の選局を制限する俗称チャンネルスキップ方式があった。そのチャンネルスキップ方式は、受信者が契約していないチャンネルを受信できないように、ＣＡＴＶ受信機が下り回線の制御情報に応じて受信可能たが、契約していないチャンネルを飛ばすものである。ところが、ＣＡＴＶチャンネル対応テレビ受像機が一般ユーザーへ販売されるようになって、チャンネルを飛ばすことができなくなり、限定受信の機能がなくなった。

【０００３】他の限定受信方式として、同期圧縮のスクランブル方式がある。この方式では、ＮＴＳＣ（Ｎａｔｉｏｎａｌ Ｔｅｌｅｖｉｓｉｏｎ Ｃｏｍｍｉｔｅｅ）映像信号の水平同期信号の期間をレベルを少なくして送信することで、ＣＡＴＶチャンネル対応テレビ受像機でも再生できなくなった。ＣＡＴＶ受信機では、受信者が契約しているチャンネルを受信する場合には、レベルが圧縮されて少なくされた水平同期信号の振幅を下り回線の制御情報、すなわちキー情報に応じてこの水平同期信号を伸長して正規のレベルまで戻すことによって、契約チャンネルを再生できる。この同期圧縮のスクランブル方式がＮＴＳＣ映像を伝送するアナログテレビジョン放送の限定受信方式として一般的であるが、デジタル有線テレビジョン放送の限定受信方式については記述されていない。

【０００４】また、最近のデジタル伝送技術などの発展に伴い、アナログ信号であるＮＴＳＣ映像の伝送チャンネル1チャンネルで複数のデジタル化された映像を伝送することが計画されている。このケーブルテレビのデジタル伝送については、１９９５年９月２１日に発表されたテレビジョン学会技術報告（ｖｏｌ．１９、Ｎｏ．４２）１９頁から２４頁の「電気通信技術審議会暫定方式デジタル有線テレビジョン放送伝送実験」に記載されている。この報告によれば、エムペグ２（ＭＰＥＧ２：Ｍｏｖｉｎｇ Ｐｉｃｔｕｒｅ Ｅｘｐｅｒｔ Ｇｒｏｕｐ ｐｈａｓｅ２）と呼ばれるデジタル画像圧縮技術によって圧縮された画像などのデジタルデータが多重されたトランスポートストリームと呼ばれる形式のデータ列にされ、リードソロモン誤り訂正などの信号処理をされた後、６４ＱＡＭ（Ｑｕａｄｒａｔｕｒｅ Ａｍｐｌｉｔｕｄｅ Ｍｏｄｕｌａｔｉｏｎ：６４値直交振幅変調）と呼ばれるデジタル変調技術によって変調されてＣＡＴＶ伝送路で伝送される。この報告でも、デジタルＣＡＴＶの限定受信方式については記述されていない。

【０００５】一方、多チャンネルのデジタル化された映像を配信する方式としてデジタル衛星テレビジョン放送があり、その放送については、日経エレクトロニクス１９９６年９月２日号１４９頁の論文「７０近くの多チャンネルを実現する日本初のデジタル衛星放送」に記載されているように、デジタル画像圧縮技術とデジタル伝送技術の組み合わせによって実現している。この論文によれば、日本独自のスクランブルシステムとＩＣカード（半導体メモリ内蔵カード）によるスクランブル解除によって、受信者を特定して受信許可する限定受信方式を実現している。このように、衛星テレビジョン放送は、衛星を介した放送のため各家庭から送信側に情報を送る上り回線は、ＩＣカードや電話回線を用いたシステムとなっている。この論文では、スクランブルシステムとＩＣカードによるスクランブル解除の限定受信方式をデジタル有線テレビジョン放送など他の伝送方式に適応するための記述が無い。

【０００６】また、ケーブルテレビのデジタルテレビジョン放送における限定受信方式については、（社）日本ＣＡＴＶ技術協会　規格・標準化委員会において標準化方式が検討され、１９９７年４月に規格書ＪＣＴＥＡ ＳＴＤ００１－１．０が発行された。それによると、この衛星テレビジョン放送に類似の方式で、送信側では映像や音声などのトランスポートストリームデータを第１の鍵データによりスクランブルし、その後第２の鍵データにより暗号化した第１の鍵データをＥＣＭ（Ｅｎｔｉｔｌｅｍｅｎｔ Ｃｏｎｔｒｏｌ Ｍｅｓｓａｇｅ）情報に入れてこれを多重器によってこの第１の鍵データによってスクランブルされた映像や音声などのトランスポートストリームデータと時分割多重する。また、第２の鍵データは第３の鍵データにより暗号化され、その後ＥＭＭ（ＥｎｔｉｔｌｅｍｅｎｔＭａｎａｇｅｍｅｎｔ Ｍｅｓｓａｇｅ）情報に入れてこれを多重器によってこの第１の鍵データによってスクランブルされた映像や音声およびこのＥＣＭ情報（以下単にＥＣＭと云う）など

のトランスポートストリームデータと時分割多重して送出する。この出力データストリームを６４ＱＡＭなどのデジタル変調する変調手段により変調し、信号合成手段により複数の被変調波を周波数多重して伝送路に送出する。ここで第３の鍵データはＩＣｶｰﾄﾞなどに記憶させておく方法などが考えられている。一方受信側では周波数多重されて伝送された６４値などの多値ＱＡＭなどのデジタル被変調波を復調手段により復調し、誤り訂正を施した後、ＭＰＥＧ分離回路で多重されているトランスポートストリームを分離する。この時ＥＣＭ情報およびＥＭＭ情報を検出し、予め与えられた第３の鍵データを用いてＥＭＭ情報（以下単にＥＭＭと云う）に含まれている第２の鍵データを復号し、復号した第２の鍵データを用いてＥＣＭ情報に含まれている第１の鍵データを復号する。この第１の鍵データを用いることでスクランブルされた映像や音声を復号することが可能となる。復号された映像や音声のトランスポートストリームはＭＰＥＧ分離回路で分離されそれぞれデコーダＩＣを通して再生される。但し、この時のＥＣＭ情報およびＥＭＭ情報のビット単位の構成に関してはなんら規定はされていない。また、送信側におけるＥＣＭ情報およびＥＭＭ情報の送出頻度も任意とされている。

【０００７】

【発明が解決しようとする課題】従来の技術では、ＣＡＴＶ伝送路を使用したデジタル有線テレビジョン放送に関する限定受信方式の詳細な技術は公開されてはいない。しかしながら現在までに規格化されている事項から考えると、ＣＡＴＶの送信側におけるＥＣＭ情報およびＥＭＭ情報の送出頻度も任意とされている。その方式によれば、受信機側に於いてスクランブルの施されたチャンネルを選ぶいわゆる選局動作をする場合には、受信機がＥＣＭ情報を受け取った時点で初めてスクランブルを解くことができるため、受信機の選局から映像や音声がスクランブルを解かれて出力するまでのいわゆる選局動作とＥＣＭ情報の送出頻度が密接に関係していた。そのため、受信機の選局動作を早くするためにはＥＣＭ情報の送出頻度を上げる必要があった。しかし、送出頻度を上げるとＥＣＭ情報の伝送容量が増えるので、同時に多重される映像や音声などのトランスポートストリームの伝送容量を圧迫してしまうといった問題が考えられる。

【０００８】本発明の目的は上記の欠点を解決したケーブルテレビの限定受信システム並びにその送信装置及びその受信装置を提供することにある。本発明の他の目的は受信装置での選局に要する時間を短縮することができるケーブルテレビの限定受信システム並びにその送信装置及びその受信装置を提供することにある。

【０００９】

【課題を解決するための手段】本発明の目的を達成するために、本発明によるケーブルテレビの限定受信システムは、第１の鍵データを第２の鍵データによって暗号化する手段、第２の鍵データを第３の鍵データによって暗号化する手段、前記暗号化された第１の鍵データによって送信するコンテンツデータをスクランブルする手段、前記スクランブル手段から取り出されたトランスポートストリーム形式の前記コンテンツデータ、暗号化された前記第１の鍵データを含むＥＣＭ情報及び暗号化された前記第２の鍵データを含むＥＭＭ情報を時分割多重する手段、前記時分割多重手段に設けられた前記ＥＣＭ情報を繰り返し出力するためのＥＣＭ記憶手段、前記時分割多重手段の出力を変調する手段を備えた送信装置と、前記デジタル変調されたコンテンツデータ、前記ＥＣＭ情報、前記ＥＭＭ情報を復調する手段、第３の鍵データの出力手段、前記ＥＣＭ情報及び復号された前記第１の鍵データのいずれか一方を記憶する第１の記憶手段、前記ＥＭＭ情報及び復号された前記第２の鍵データのいずれか一方を記憶する第２の記憶手段、暗号化された前記第２の鍵データを前記第３の鍵データを用いて復号する第２の鍵データ復号手段、暗号化された前記第１の鍵データを前記復号された第２の鍵データを用いて復号する第１の鍵データ復号手段、復号された前記第１の鍵データを用いて前記コンテンツデータのスクランブルを解除する手段を備え、前記第１、前記第２の記憶手段の出力を用いてスクランブルを解除する受信装置と、から構成される。

【００１０】このケーブルテレビの限定受信システムにおいて、前記送信装置の前記時分割多重手段にＥＭＭ情報を繰り返し出力するためのＥＭＭ記憶手段を設ける。また、このケーブルテレビの限定受信システムにおいて、前記受信装置の前記第１の記憶手段はＥＣＭ情報を記憶し、前記第２の記憶手段はＥＭＭ情報を記憶する。また、このケーブルテレビの限定受信システムにおいて、前記受信装置の前記第１の記憶手段は復号された第１の鍵データを記憶し、前記第２の記憶手段は復号された第２の鍵データを記憶する。また、このケーブルテレビの限定受信システムにおいて、前記受信装置の前記第１の記憶手段にはＥＣＭ情報を記憶し、前記第２の記憶手段には復号された第２の鍵データを記憶する。

【００１１】本発明の目的を達成するために、本発明のケーブルテレビの送信装置は、第１の鍵データを第２の鍵データによって暗号化する手段と、第２の鍵データを第３の鍵データによって暗号化する手段と、暗号化された前記第１の鍵データによって送信するコンテンツデータをスクランブルする手段と、前記スクランブル手段から取り出されたトランスポートストリーム形式の前記コンテンツデータ、暗号化された前記第１の鍵データを含むＥＣＭ情報及び暗号化された前記第２の鍵データを含むＥＭＭ情報を時分割多重手段と、前記時分割多重手段に設けられ、前記ＥＣＭ情報を繰り返し出力するためのＥＣＭ記憶手段と、前記時分割多重手段の出力を変調して送信する手段とを備えている。また、この送信装置に

おいて、前記送信装置の前記時分割多重手段に前記ＥＭＭ情報を繰り返し出力するためのＥＭＭ記憶手段を設ける。

【００１２】本発明の目的を達成するために、本発明のケーブルテレビ受信装置は、送信装置から送付されたスクランブルされたコンテンツデータ、ＥＣＭ情報、ＥＭＭ情報からコンテンツデータのスクランブルを解除するために、第３の鍵データの出力手段と、前記ＥＣＭ情報及び復号された前記第１の鍵データのいずれか一方を記憶する第１の記憶手段と、前記ＥＭＭ情報及び復号された前記第２の鍵データのいずれか一方を記憶する第２の記憶手段と、暗号化された前記第２の鍵データを前記第３の鍵データを用いて復号する第２の鍵データ復号手段と、暗号化された前記第１の鍵データを前記復号された第２の鍵データを用いて復号する第１の鍵データ復号手段と、復号された前記第１の鍵データを用いて前記コンテンツデータのスクランブルを解除する手段を備え、前記第１、前記第２の記憶手段の出力を用いてスクランブルを解除する。

【００１３】このケーブルテレビの限定受信システムにおいて、前記受信装置の前記第１の記憶手段は前記ＥＣＭ情報を記憶し、前記第２の記憶手段は前記ＥＭＭ情報を記憶する。また、このケーブルテレビの受信装置において、前記受信装置の前記第１の記憶手段は復号された第１の鍵データを記憶し、前記第２の記憶手段は復号された第２の鍵データを記憶する。また、このケーブルテレビの受信装置において、前記受信装置の前記第１の記憶手段はＥＣＭ情報を記憶し、前記第２の記憶手段は復号された第２の鍵データを記憶する。また、このケーブルテレビの受信装置において、前記第１の記憶手段の出力を用いて前記スクランブル解除手段でコンテンツデータのスクランブルが解除されない場合には、送信されてきたＥＣＭ情報を用いて前記第１の記憶手段を更新し、前記第１の記憶手段の出力を用いてコンテンツデータのスクランブルを解除する。また、このケーブルテレビの受信装置において、前記第２の記憶手段の出力を用いて前記第１の鍵データの復号ができない場合には、送信されてきたＥＭＭ情報で前記第２の記憶手段を更新し、前記更新された第２の記憶手段の出力を用いて前記第１の鍵データを復号する。

【００１４】本発明の目的を達成するために、本発明によるケーブルテレビの限定受信システムは、トランスポートストリーム形式のデジタルデータを暗号化して伝送するケーブルテレビシステムにおいて、映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段、受信側でコンテンツのスクランブルを解除するために必要となる第１の鍵データの暗号化されたデータを含むＥＣＭ情報を生成しスクランブル装置を制御するスクランブル制御装置、前記第１の鍵データの暗号化を解除する場合に必要となる第２の鍵データを含むＥＭＭ情報を生成する限定受信制御装置、第２の鍵データの暗号化を解除するために必要となる第３の鍵データ及び前記第１、前記第２の鍵データ及び顧客情報を管理する鍵情報管理装置、トランスポートストリーム形式のデジタルデータと前記ＥＣＭ情報や前記ＥＭＭ情報を時分割多重すると共に前記ＥＣＭ情報及び前記ＥＭＭ情報を記憶して繰り返し送出する機能を有する多重化装置、前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段、複数の被変調波を周波数多重して伝送路に送出する信号合成手段を備えた送信装置と、周波数多重されて伝送されたデジタル被変調波を復調する復調手段、前記復調手段で得られた前記ＥＣＭ情報より前記第１の鍵データを復号する第１の鍵データ復号手段、前記復調手段で得られた前記ＥＭＭ情報より前記第２の鍵データを復号する第２の鍵データ復号手段、前記ＥＣＭ情報を対応する契約チャンネル毎に記憶するＥＣＭ記憶手段、前記ＥＭＭ情報を対応する契約チャンネル毎に記憶するＥＭＭ記憶手段、前記復調手段で得られたコンテンツスクランブルのかかった前記データから前記第１の鍵データ復号手段で得られた第１の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段、を備えた受信装置と、から構成され、ＥＣＭ情報に変更があるまでは契約チャンネルを選局する毎に前記ＥＣＭ記憶手段に記憶したＥＣＭ情報を利用して、このデータを一旦前記第１の鍵データ復号手段において復号することにより前記第１の鍵データを抽出し、この抽出した前記第１の鍵データを用いて前記復調手段で得られたコンテンツスクランブルのかかった前記データより前記デスクランブル手段によって前記トランスポートストリーム形式のデジタルデータを得る。

【００１５】また、本発明による限定受信システムは、トランスポートストリーム形式のデジタルデータを暗号化して伝送するケーブルテレビシステムにおいて、映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段、受信側でコンテンツのスクランブルを解除するために必要となる第１の鍵データの暗号化されたデータを含むＥＣＭ情報を生成しスクランブル装置を制御するスクランブル制御装置、前記第１の鍵データの暗号化を解除する場合に必要となる第２の鍵データを含むＥＭＭ情報を生成し多重化装置へ出力する限定受信制御装置、前記第２の鍵データの暗号化を解除するために必要となる第３の鍵データ、前記第１、前記第２の鍵データ及び顧客情報を管理する鍵情報管理装置、トランスポートストリーム形式のデジタルデータと前記ＥＣＭ情報や前記ＥＭＭ情報を時分割多重すると共に前記ＥＣＭ情報及び前記ＥＭＭ情報を記憶して繰り返し送出する機能を有する多重化装置、前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段、複数の被変調波を周波数多重

して伝送路に送出する信号合成手段、とを備えた送信装置と、周波数多重されて伝送されたデジタル被変調波を復調する復調手段と、前記復調手段で得られた前記ＥＣＭ情報より前記第１の鍵データを復号する第１の鍵データ復号手段、前記復調手段で得られた前記ＥＭＭ情報より前記第２の鍵データを復号する第２の鍵データ復号手段、前記第１の鍵データ復号手段によって復号された前記第１の鍵データ自体を対応する契約チャンネル毎に記憶する第１の鍵データ記憶手段、前記第２の鍵データ復号手段によって復号された前記第２の鍵データ自体を対応する契約チャンネル毎に記憶する第２の鍵データ記憶手段、前記復調手段で得られたコンテンツスクランブルのかかったデータから前記ＥＣＭ復号手段から得られた復号化された前記第１の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段、とを備えた受信装置と、から構成され、前記ＥＣＭ情報または前記ＥＭＭ情報に変更があるまでは前記鍵データ記憶手段に記憶された鍵データを利用して前記デスクランブル手段によって前記復調手段で得られたコンテンツスクランブルのかかったデータからトランスポートストリーム形式のデジタルデータを得る。

【００１６】本発明によるケーブルテレビの送信装置は、暗号化されたトランスポートストリーム形式のデジタルデータを送信するために、映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段と、受信側でコンテンツのスクランブルを解除するために必要となる第１の鍵データの暗号化されたデータを含むＥＣＭ情報を生成しスクランブル装置を制御するスクランブル制御装置と、前記第１の鍵データの暗号化を解除する場合に必要となる第２の鍵データを含むＥＭＭ情報を生成し多重化装置へ出力する限定受信制御装置と、前記第２の鍵データの暗号化を解除するために必要となる第３の鍵データ、前記第１、前記第２の鍵データ及び顧客情報を管理する鍵情報管理装置と、トランスポートストリーム形式のデジタルデータと前記ＥＣＭ情報や前記ＥＭＭ情報を時分割多重すると共に前記ＥＣＭ情報及び前記ＥＭＭ情報を記憶して繰り返し送出する機能を有する多重化装置と、前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段と、複数の被変調波を周波数多重して伝送路に送出する信号合成手段とを備えている。

【００１７】本発明によるケーブルテレビの受信装置は、周波数多重されて伝送されたデジタル被変調波を復調する復調手段と、前記復調手段で得られたＥＣＭ情報より第１の鍵データを復号する第１の鍵データ復号手段と、前記復調手段で得られたＥＭＭ情報より第２の鍵データを復号する第２の鍵データ復号手段と、前記ＥＣＭ情報を対応する契約チャンネル毎に記憶するＥＣＭ記憶手段と、前記ＥＭＭ情報を記憶するＥＭＭ記憶手段と、前記復調手段で得られたコンテンツスクランブルのかかったデータから前記第１の鍵データ復号手段で得られた第１の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段とを備えている。

【００１８】このケーブルテレビの受信装置において、前記受信装置が映像や音声の選択をするためのいわゆる選局動作をする場合、まず前記ＥＣＭ記憶手段に記憶されたＥＣＭ情報を用いて前記第１の鍵データを復号して前記デスクランブル手段に供給し、前記第１の鍵データでデスクランブル処理がされない場合には前記復調手段から新しくＥＣＭ情報を抽出して前記ＥＣＭ記憶手段に記憶されたＥＣＭ情報を更新し、更新されたＥＣＭ情報によって第１の鍵データを復号して前記デスクランブル手段に供給してスクランブル解除する。

【００１９】本発明によるケーブルテレビの受信装置は、周波数多重されて伝送されたデジタル被変調波を復調する復調手段と、前記復調手段で得られたＥＣＭ情報より第１の鍵データを復号する第１の鍵データ復号手段と、前記復調手段で得られたＥＭＭ情報より第２の鍵データを復号する第２の鍵データ復号手段と、前記第１の鍵データ復号手段によって復号された前記第１の鍵データ自体を対応する契約チャンネル毎に記憶する第１の鍵データ記憶手段と、前記第２の鍵データ復号手段によって復号された前記第２の鍵データ自体を対応する契約チャンネル毎に記憶する第２の鍵データ記憶手段と、前記復調手段で得られたコンテンツスクランブルのかかったデータから前記ＥＣＭ復号手段で得られた鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段とを備えている。

【００２０】このケーブルテレビの受信装置において、前記受信装置が映像や音声の選択をするためのいわゆる選局動作をする場合、まず前記第１の鍵データ記憶手段に記憶された前記第１の鍵データを前記デスクランブル手段に用い、デスクランブル処理がされない場合には前記復調手段から新しくＥＣＭ情報を抽出して前記第１の鍵データ復号手段によって第１の鍵データを復号して前記第１の鍵データ記憶手段に記憶された第１の鍵データを更新し、前記更新された第１の鍵データを前記デスクランブル手段に供給してスクランブルを解除する。

【００２１】本発明によるケーブルテレビの限定受信システムは、トランスポートストリーム形式のデジタルデータを暗号化して伝送するケーブルテレビシステムにおいて、映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段、受信側でコンテンツのスクランブルを解除するために必要となる第１の鍵データの暗号化されたデータを含むＥＣＭ情報を生成しスクランブル装置を制御するスクランブル制御装置、前記第１の鍵データの暗号化を解除する場合に必要となる第２の鍵データを含むＥＭＭ情報を生成し多重化装置へ出力する限定受信制御装置、前記

第２の鍵データの暗号化を解除するために必要となる第３の鍵データ、前記第１、前記第２の鍵データ及び顧客情報を管理する鍵情報管理装置、トランスポートストリーム形式のデジタルデータと前記ＥＣＭ情報や前記ＥＭＭ情報を時分割多重すると共に前記ＥＣＭ情報を記憶して繰り返し送出する機能を有する多重化装置、前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段、複数の被変調波を周波数多重して伝送路に送出する信号合成手段、とを備えた送信装置と、周波数多重されて伝送されたデジタル被変調波を復調する復調手段、前記復調手段で得られた前記ＥＣＭ情報より前記第１の鍵データを復号する第１の鍵データ復号手段、前記復調手段で得られた前記ＥＭＭ情報より前記第２の鍵データを復号する第２の鍵データ復号手段、前記ＥＣＭ情報を対応する契約チャンネル毎に記憶するＥＣＭ記憶手段、前記ＥＭＭ情報を対応する契約チャンネル毎に記憶するＥＭＭ記憶手段、前記復調手段で得られたコンテンツスクランブルのかかったデータから前記第１の鍵データ復号手段で得られた前記第１の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段、とを備えた受信装置と、から構成され、前記ＥＣＭ情報に変更があるまでは契約チャンネルを選局する毎に前記ＥＣＭ記憶手段に記憶した前記ＥＣＭ情報を利用するために、このデータを一旦前記第１の鍵データ復号手段で復号して前記第１の鍵データを抽出し、この抽出された前記第１の鍵データを用いて前記復調手段で得られたコンテンツスクランブルのかかったデータより前記デスクランブル手段によってトランスポートストリーム形式のデジタルデータを得る。

【００２２】本発明によるケーブルテレビの限定受信システムは、トランスポートストリーム形式のデジタルデータを暗号化して伝送するケーブルテレビシステムにおいて、映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段、受信側でコンテンツのスクランブルを解除するために必要となる第１の鍵データの暗号化されたデータを含むＥＣＭ情報を生成しスクランブル装置を制御するスクランブル制御装置、前記第１の鍵データの暗号化を解除する場合に必要となる第２の鍵データを含むＥＭＭ情報を生成し多重化装置へ出力する限定受信制御装置、前記第２の鍵データの暗号化を解除するために必要となる第３の鍵データ、前記第１、前記第２の鍵データ及び顧客情報を管理する鍵情報管理装置、トランスポートストリーム形式のデジタルデータと前記ＥＣＭ情報や前記ＥＭＭ情報を時分割多重すると共に前記ＥＣＭ情報を記憶して繰り返し送出する機能を有する多重化装置、前記スクランブル制御装置の出力データストリームをデジタル変調する変調手段、複数の被変調波を周波数多重して伝送路に送出する信号合成手段、とを備えた送信装置と、周波数多重されて伝送されたデジタル被変調波を復調する復調手段、前記復調手段で得られた前記ＥＣＭ情報より前記第１の鍵データを復号する第１の鍵データ復号手段、前記復調手段で得られた前記ＥＭＭ情報より前記第２の鍵データを復号する第２の鍵データ復号手段、前記ＥＣＭ情報を対応する契約チャンネル毎に記憶するＥＣＭ記憶手段、前記第２の鍵データ復号手段によって復号された前記第２の鍵データ自体を対応する契約チャンネル毎に記憶する第２の鍵データ記憶手段、前記復調手段で得られたコンテンツスクランブルのかかったデータから前記第１の鍵データ復号手段で得られた前記第１の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段、を備えた受信装置と、から構成され、前記ＥＣＭ情報に変更があるまでは契約チャンネルを選局する毎に前記ＥＣＭ記憶手段に記憶した前記ＥＣＭ情報を利用すると共に、前記ＥＭＭ情報に変更があるまでは前記鍵データ記憶手段に記憶された鍵データを利用するために、このデータを一旦前記第１の鍵データ復号手段で復号して前記第１の鍵データを抽出し、この抽出された前記第１の鍵データを用いて前記復調手段で得られたコンテンツスクランブルのかかったデータより前記デスクランブル手段によってトランスポートストリーム形式のデジタルデータを得る。

【００２３】本発明によるケーブルテレビの受信装置は、周波数多重されて伝送されたデジタル被変調波を復調する復調手段と、前記復調手段で得られたＥＣＭ情報より第１の鍵データを復号する第１の鍵データ復号手段と、前記復調手段で得られたＥＭＭ情報より第２の鍵データを復号する第２の鍵データ復号手段と、前記ＥＣＭ情報を対応する契約チャンネル毎に記憶するＥＣＭ記憶手段と、前記第２の鍵データ復号手段によって復号された前記第２の鍵データ自体を対応する契約チャンネル毎に記憶する第２の鍵データ記憶手段と、前記復調手段で得られたコンテンツスクランブルのかかったデータから前記第１の鍵データ復号手段で得られた第１の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段とを備える。このケーブルテレビの受信装置において、前記受信装置が映像や音声の選択をするためのいわゆる選局動作をする場合、まず前記ＥＣＭ記憶手段に記憶されたＥＣＭ情報を用いて前記第１の鍵データを復号して前記デスクランブル手段に用い、デスクランブル処理がされない場合には前記復調手段から新しくＥＣＭ情報を抽出して前記ＥＣＭ記憶手段に記憶された前記ＥＣＭ情報を更新し、その更新されたＥＣＭ情報によって第１の鍵データを復号して前記デスクランブル手段に供給してスクランブル解除をする。

【００２４】また、上記目的を達成するために、本発明においては、送信側では映像や音声又は他のデータをトランスポートストリームとして出力するトランスポートストリーム出力手段とコンテンツのスクランブルを解除するために必要となる第１の鍵データを含むＥＣＭ情報

を生成しスクランブル装置を制御するスクランブル制御装置と同じくコンテンツのスクランブルを解除するために必要となる第２の鍵データを含むＥＭＭ情報を生成し多重化装置へ出力する限定受信制御装置とトランスポートストリーム形式のデジタルデータとＥＣＭ情報やＥＭＭ情報を時分割多重すると共に前記ＥＣＭ情報を記憶して繰り返し送出する機能を有する多重化装置と前記スクランブル制御装置の出力データストリームを６４値などの多値ＱＡＭなどのデジタル変調する変調手段と複数の被変調波を周波数多重して伝送路に送出する信号合成手段とを備え、受信側では周波数多重されて伝送された６４値などの多値ＱＡＭなどのデジタル被変調波を復調する復調手段と、前記復調手段で得られたＥＣＭ情報を対応する契約チャンネル毎に記憶するＥＣＭ記憶手段と前記ＥＣＭ情報の中から第１の鍵データを復号する第１の鍵データ復号手段と前記復調手段で得られたＥＭＭ情報を対応する契約チャンネル毎に記憶するＥＭＭ記憶手段と前記ＥＭＭ情報の中から第２の鍵データを復号する第２の鍵データ復号手段と予めトランスポートストリームとは別の経路によって与えられる第３の鍵データ記憶手段と前記復調手段で得られたコンテンツスクランブルのかかったデータから前記第１の鍵データ復号手段によって得られた第１の鍵データによってトランスポートストリーム形式のデジタルデータを得るデスクランブル手段とを備える。

【００２５】ＥＣＭ情報に変更があるまでは契約チャンネルを選局する毎に前記ＥＣＭ記憶手段に記憶したＥＣＭ情報を利用して前記第１の鍵データを抽出できる。また、ＥＣＭ情報が変更された場合など、前記ＥＣＭ記憶手段に記憶したＥＣＭ情報を利用してデスクランブル処理ができない場合には、復調手段から新しくＥＣＭ情報を抽出して更新して利用できる。ＥＭＭデータを一旦前記第２の鍵データ復号手段において復号することにより前記第２の鍵データを、ＥＣＭデータを一旦前記第１の鍵データ復号手段において復号することにより前記第１の鍵データを抽出できる。このＥＣＭ記憶手段に記憶したＥＣＭ情報より抽出した第１の鍵データを用いて前記デスクランブル手段によってデスクランブルすることで選局時間を短縮することができる。また、ＥＣＭ情報やＥＭＭ情報の更新頻度や送信頻度を低くした場合にも選局時間の短縮が可能である。

【００２６】

【発明の実施の形態】以下本発明によるケーブルテレビの限定受信システム並びにその送信装置及びその受信装置の実施の形態について、実施例を用い、図面を参照して説明する。

【００２７】図１は本発明によるケーブルテレビの限定受信システム並びにその送信装置及びその受信装置の一実施例を示すブロック図である。図１において、１００は送信側暗号化変調装置、２００はＭＰＥＧ圧縮装置や音声信号や映像信号を記憶しておくサーバなどを有する送信側映像信号源装置、３００は暗号化鍵や顧客を管理するための送信側鍵等管理装置、４００はＣＡＴＶ伝送路、５００は受信側端末装置、６００は映像音声表示器、７００は郵送などの配送手段である。暗号化装置１０１は映像音声多重化及びコンテンツスクランブル回路１１１、１１２はスクランブル制御装置１１２、限定受信制御装置１１３から構成されている。時分割多重回路１０２はＥＣＭ記憶回路１２１、ＥＭＭ記憶回路１２２から構成されている。１０３は６４ＱＡＭ（Ｑｕａｄｒａｔｕｒｅ ＡｍｐｌｉｔｕｄｅＭｏｄｕｌａｔｉｏｎ）変調回路、１０４は信号合成回路である。１５１は映像音声データ出力端子、１５２は第１の鍵データ出力端子、１５３は第２の鍵データ出力端子、１５４は第３の鍵データ出力端子、１５５は暗号化された第１の鍵データを含むＥＣＭ（Ｅｎｔｉｔｌｅｍｅｎｔ Ｃｏｎｔｒｏｌ Ｍｅｓｓａｇｅ）情報出力端子、１５６は暗号化された第２の鍵データを含むＥＭＭ（Ｅｎｔｉｔｌｅｍｅｎｔ Ｍａｎａｇｅｍｅｎｔ Ｍｅｓｓａｇｅ）情報出力端子、１５７はスクランブル映像音声データ出力端子、１５８はスクランブル映像音声、ＥＣＭ情報、ＥＭＭ情報多重データ出力端子、１５９は６４ＱＡＭデジタル被変調波信号出力端子である。５０１は周波数多重信号分離回路、５０２は制御用マイコン、５０３は６４ＱＡＭ復調回路、５０４は誤り訂正回路、５０８はコンテンツデスクランブル回路、５０９はＭＰＥＧ多重分離回路、５１０はＭＰＥＧビデオデコーダ、５１１はＮＴＳＣ（Ｎａｔｉｏｎａｌ ＴｅｌｅｖｉｓｉｏｎＳｙｓｔｅｍ Ｃｏｍｍｉｔｔｅｅ）ビデオエンコーダ、５１２はオーディオデコーダ、５１３はＩＣカードなどの情報記憶媒体、５１４はＥＣＭ記憶手段、５１５はＥＭＭ記憶手段、５０５は鍵情報分離回路、５０６は第2の鍵復号回路、５０７は第1の鍵復号回路である。５５１は制御信号出力端子、５５２は６４ＱＡＭ被変調波信号出力端子、５５３は６４ＱＡＭ復調デジタルデータ出力端子、５５５は誤り訂正後デジタルデータ出力端子、５５６は暗号化された第１の鍵データ出力端子、５５７は暗号化された第２の鍵データ出力端子、５５８は第３の鍵データ出力端子、５５９は第２の鍵データ出力端子、５６０は第１の鍵データ出力端子、５６１はデスクランブルデジタルデータ出力端子、５６８はＥＭＭ情報出力端子、５６９はＥＣＭ情報出力端子、５６２は圧縮映像データ出力端子、５６４は映像データ出力端子、５６３は圧縮オーディオデータ出力端子、５６５はＮＴＳＣビデオ信号出力端子、５６６はアナログオーディオ信号出力端子である。

【００２８】限定受信方式を有したケーブルテレビの送信装置は、送信側暗号化変調装置１００、送信側映像信号源装置２００および送信側鍵等管理装置３００で構成され、送信側映像信号源装置２００からの映像や音声の

データを含んだ映像音声データはＭＰＥＧ2トランスポートストリーム形式あるいはトランスポートストリームに変換可能な形式のデジタルデータであり、端子１５１から暗号化装置１０１の映像音声多重化及びコンテンツスクランブル回路１１１に入力される。映像音声データは映像音声多重化及びコンテンツスクランブル回路１１１で送信側鍵等管理装置３００から出力された第１の鍵データによってトランスポートストリーム形式のデジタルデータを暗号化したスクランブル映像音声データとして端子１５７に出力され、時分割多重回路１０２に供給される。送信側鍵等管理装置３００は第１の鍵データ１５２をスクランブル制御装置１１２へ送出し、第２の鍵データ１５３及び第３の鍵データ１５４を限定受信制御装置１１３へ送出する。スクランブル制御装置１１３は送信側鍵等管理装置３００より受信した第１の鍵データ１５２を映像音声多重化及びコンテンツスクランブル回路１１１へ送出すると共に限定受信制御装置１１３より送られてくる第２の鍵データ１５３によって第１の鍵データ１５２を暗号化した後ＥＣＭ情報の一部として時分割多重回路１０２へ送出する。この時第１の鍵データをスクランブル制御装置１１３に供給し、タイミングを制御しながら映像音声多重化及びコンテンツスクランブル回路１１１に供給しても良い。送信側鍵等管理装置３００の端子１５３から取り出された第２の鍵データはスクランブル制御装置１１２に送出されると共に限定受信制御装置１１３に供給される。限定受信制御装置１１３において、第２の鍵データは送信側鍵等管理装置３００の出力端子１５４から送られてくる第３の鍵データによって第２の鍵データを暗号化した後ＥＭＭ情報の一部として時分割多重回路１０２へ送出する。時分割多重回路１０２には、端子１５５に取り出されたＥＣＭ情報を記憶するＥＣＭ記憶回路１２１と端子１５６に取り出されたＥＭＭ情報を記憶するＥＭＭ記憶回路１２２とが設けられており、それぞれの情報が更新されるまでは一旦記憶した情報を保持し、設定されたタイミングでＥＣＭ記憶回路１２１とＥＭＭ記憶回路１２２に記憶された情報である暗号化された第１の鍵データを含むＥＣＭ情報、暗号化された第２の鍵データを含むＥＭＭ情報とスクランブル映像音声データをトランスポートストリーム形式のデジタルデータとして時分割多重して、時分割多重装置１０２の端子１５８にスクランブル映像音声ＥＣＭ情報、ＥＭＭ情報多重データとして６４ＱＡＭ変調回路１０３に加えられる。なお、このＥＣＭ情報、ＥＭＭ情報は鍵情報だけを含む場合と、鍵情報のほかに他の情報、例えば契約情報などが含まれる場合がある。この他の情報は図示しない回路からスクランブル制御装置１１２及び限定受信制御装置１１３に供給される。

【００２９】６４ＱＡＭ変調回路１０３ではスクランブル映像音声ＥＣＭ情報、ＥＭＭ情報多重データに誤り訂正用符号を付加し、インターリーブ処理及びエネルギー拡散処理などをが行なわれ、６４ＱＡＭデジタル被変調波信号に変換されて端子１５９に出力される。この６４ＱＡＭデジタル被変調波信号は信号合成回路１０４で他の６４ＱＡＭデジタル被変調波信号やアナログ被変調波信号などと周波数多重されてＣＡＴＶ伝送路４００に出力される。第３の鍵データ１５４は、ＩＣカード等の情報記憶媒体５１３などによって郵送などの配送手段によって線路７００を経由して限定受信方式を有したケーブルテレビの受信装置に配られる。

【００３０】一方、限定受信方式を有したケーブルテレビの受信装置は、受信側端末装置５００で構成される。受信側端末装置５００では、周波数多重されて伝送された６４ＱＡＭデジタル被変調波信号をＣＡＴＶ伝送路４００から受ける。選局などの制御を行う制御用マイコン５０２の端子５５１に取り出された制御信号によって、この信号は周波数多重信号分離回路５０１で選局され、６４ＱＡＭ被変調波信号として端子５５２に取り出され、６４ＱＡＭ復調回路５０３に入力される。６４ＱＡＭ復調回路５０３で６４ＱＡＭ被変調波信号は６４ＱＡＭ復調デジタルデータに復調され、端子５５３を介して誤り訂正回路５０４に供給され、ここで、伝送路で生じたデータの誤りが訂正される。誤り訂正後のデジタルデータは端子５５５を介してコンテンツデスクランブル回路５０８に入力される。誤り訂正回路５０４ではインターリーブ処理やエネルギー拡散処理されたデータの復号も行なわれる。第１の鍵データ５６０が復号されるまではコンテンツデスクランブル回路５０８においてデスクランブルは実行されず、誤り訂正後デジタルデータはそのままＭＰＥＧ分離回路５０９へ入力される。ＭＰＥＧ分離回路５０９ではトランスポートストリーム形式で送られてきたＥＣＭ情報及びＥＭＭ情報を検出し、それぞれ端子５６９、５６８を通してＥＣＭ記憶手段５１４及びＥＭＭ記憶手段５１５へと送出される。ＥＣＭ記憶手段５１４に記憶されたＥＣＭ情報とＥＭＭ記憶手段５１５に記憶されたＥＭＭ情報は必要に応じて鍵情報分離回路５０５に送られる。鍵情報分離回路５０５は記憶されていたＥＣＭ情報より暗号化された第１の鍵データを抽出して端子５５６に出力し、第１の鍵復号回路５０７へ送出する。また鍵情報分離回路５０５は記憶されていたＥＭＭ情報より暗号化された第２の鍵データ５５７を抽出して端子５５７に出力し、第２の鍵復号回路５０６へ送出する。第2の鍵復号回路５０６では、郵送などの配送手段によって線路７００を経由して入手したＩＣカード等の情報記憶媒体５１３からの第３の鍵データを端子５５８に出力し、これによって暗号化された第２の鍵データを復号して端子５５９に第２の鍵データが得られる。第２の鍵データを第１の鍵復号回路５０７に供給することによって、第２の鍵データで暗号化された第１の鍵データを復号して端子５６０に第１の鍵データを得る。コンテンツデスクランブル回路５０８では、端子５

６０から得られた第１の鍵データによって、暗号化されている誤り訂正後デジタルデータを復号して、ＭＰＥＧ2トランスポートストリーム形式のデスクランブルデジタルデータ５６１に戻す。ＭＰＥＧ多重分離回路５０９では圧縮映像データと圧縮オーディオデータに分離され、端子５６２には圧縮映像データが得られ、端子５６３には圧縮オーディオデータがえられ、それぞれＭＰＥＧビデオデコーダ５１０とオーディオデコーダ５１２に入力される。圧縮映像データはＭＰＥＧビデオデコーダ５１０によって映像データに変換され端子５６４に取り出され、ＮＴＳＣビデオエンコーダ５１１によってＮＴＳＣビデオ信号に変換され、端子５６５からとりだされる。ＭＰＥＧ分離回路５０９の端子５６３に取り出された圧縮オーディオデータはオーディオデコーダ５１２に供給され、ここでアナログオーディオ信号に変換されて端子５６６に取り出される。このＮＴＳＣビデオ信号とアナログオーディオ信号は映像音声表示器６００に入力されて、映像音声表示器６００で表示された映像と音声などの情報を視聴者に提供できる。

【００３１】以上のように、図１に示す実施例では、視聴者が契約したチャンネルを見る場合には、受信側端末装置５００内部のＥＣＭ記憶手段５１４及びＥＭＭ記憶手段５１５に記憶してあるＥＣＭ情報や記憶してあるＥＭＭ情報を用いることによって、直ちに記憶してある暗号化された第１の鍵データ５５６を復号して、復号された第１の鍵データを得ることができる。従って、番組選択の都度あらためてＥＣＭ情報やＥＭＭ情報を検出する必要はなく、その時間分だけ早く、コンテンツスクランブルを施した誤り訂正後デジタルデータをコンテンツデスクランブル回路５０８で復号して、ＭＰＥＧ2トランスポートストリーム形式のデスクランブルデジタルデータに戻すことができ、短時間で表示された映像と音声などの情報を得ることができる。

【００３２】なお、本実施例において、電源投入とともにＥＣＭ記憶手段５１４に全てのＥＣＭ情報が記憶され、ＥＭＭ記憶手段５１５に全てのＥＭＭ情報が記憶されるようにすることによって、第１の鍵データ、第２の鍵データを短時間で得ることが出来る。

【００３３】また、選局要求に従って前記ＥＣＭ記憶手段５１４に記憶されているＥＣＭ情報より第１の鍵復号回路５０７によって復号された第１の鍵データを使用してコンテンツデスクランブル回路５０８でデスクランブルを行ってもスクランブルが解除できない場合には、改めてＭＰＥＧ分離回路５０９よりＥＣＭ情報を抽出し、ＥＣＭ記憶手段５１４の記憶内容を更新すると共に、鍵情報分離回路５０５を通して第１の鍵復号回路５０７により得られた暗号化された第１の鍵データを第２の鍵データで復号することによって、コンテンツデスクランブル回路５０８においてデスクランブルが可能となる。一方、送信側でＥＣＭ情報やＥＭＭ情報が更新され、受信側端末装置５００内部に記憶された更新前のＥＣＭ情報やＥＭＭ情報が使用できなくなった場合には、時分割多重回路１０２においてＥＣＭ情報やＥＭＭ情報の送出頻度を上げておけば比較的短時間で受信側端末装置５００でＥＣＭ情報やＥＭＭ情報を検出することができる。

【００３４】なお、本実施例では、第１の鍵データから第３の鍵データまでの３種類の鍵データを用いたが、鍵の数には関係無く送信側鍵等管理装置３００より更新及び送信される鍵の記憶・復号手段を受信側端末装置５００内部に設けることによって短時間で選局動作を行うデジタル有線テレビジョン放送の限定受信方式を実現できる。一般的には、その鍵の数を増やすほど盗聴できにくいと言われている。

【００３５】なお、本発明の実施例において、制御用マイコン５０２はＥＣＭ情報やＥＭＭ情報が暗号化されているか否か、ＥＣＭ情報やＥＭＭ情報が周波数多重分離回路５０１に入力されたか否かを監視すると共に画面上での契約状況が確認できるよう制御することができる。

【００３６】図２は本発明によるケーブルテレビの限定受信システムに使用されるＭＰＥＧ2トランスポートストリーム形式の信号構成を示す概念図である。図２において、２００1はパケットヘッダであり、２００２はＭＰＥＧ映像データや音声データであり、ＥＣＭ情報やＥＭＭ情報が含まれている。また、１チャンネルに複数、例えば４つの番組が多重されており、この番組を識別するためにＳＩ情報が用いられる。２００3は誤り訂正符号を示す。受信側端末装置５００のＭＰＥＧ2トランスポートストリーム形式に戻されたデスクランブルデジタルデータのデータの構成は、４バイトのパケットヘッダ２００1と１８４バイトのＭＰＥＧ映像データやＭＰＥＧ音声データおよびＥＣＭ情報やＥＭＭ情報のパケット２００２で構成される。この４ビットのパケットヘッダ２００１と１８４バイトのパケット２００２で構成される１８８バイトのＭＰＥＧ2トランスポートストリーム形式のデータに１６バイトのリードソロモンと呼ばれる誤り訂正符号２００3が付加されている。

【００３７】図３は本発明によるケーブルテレビの限定受信システムに使用されるＭＰＥＧ2トランスポートストリーム形式のパケットヘッダの信号構成を示す概念図である。図３において、３００1は同期バイト、３００２はトランスポートエラーインジケータ、３００３はペイロードユニット開始インジケータ、３００４はトランスポート優先度、３００５はパケット識別子、３００６はトランスポートスクランブル制御、３００７はアダプテーションフィールド制御、３００８は連続性指標を示す。図３は図２に示す４バイトのパケットヘッダ２００１の詳細を示すもので、ＭＰＥＧデータ２００２に記載されるＭＰＥＧ映像データやＭＰＥＧ音声データおよびＥＣＭ情報やＥＭＭ情報等のデータの内、特定の情報のパケットを検出するためのパケット識別子３００５やこ

のＭＰＥＧ映像データパケットにスクランブルが施されているかを示すトランスポートスクランブル制御３００６などが付加されたものである。

【００３８】図４は本発明によるケーブルテレビの限定受信システム並びにその送信装置及びその受信装置の他の実施例を示すブロック図である。図４において、５２０は第２の鍵データ記憶手段、５２１は第１の鍵データ記憶手段である。５７３は第２の鍵データ記憶手段５２０の出力端子であり、この端子５７３に記憶された第２の鍵データが出力される。５７２は第１の鍵データ記憶手段５２１の出力端子であり、この端子５７２に第１の鍵データ記憶手段５２１記憶された第１の鍵データが出力される。なお、図４において、図１と同じ機能を有するブロックには同一の符号を付けている。

【００３９】受信側端末装置５００では、周波数多重されて伝送された６４ＱＡＭデジタル被変調波信号をＣＡＴＶ伝送路４００から受け、周波数多重信号分離回路５０１で制御用マイコン５０２からの制御信号に応じて６４ＱＡＭ被変調波信号を選局する。この被変調波信号は６４ＱＡＭ復調回路５０３に入力される。６４ＱＡＭ復調回路５０３で６４ＱＡＭ被変調波信号は６４ＱＡＭ復調デジタルデータに復調され、端子５５３を通して誤り訂正回路５０４に供給され、この回路５０４で伝送路で生じたデータの誤りが訂正され、誤り訂正後デジタルデータとして端子５５５を通してコンテンツデスクランブル回路５０８に入力される。

【００４０】誤り訂正回路５０４では、インターリーブ処理やエネルギー拡散処理されたデータの復号も行なう。第１の鍵データ５６０が復号されるまではコンテンツでスクランブル回路５０８においてデスクランブルは実行されず誤り訂正後デジタルデータはそのままＭＰＥＧ分離回路５０９へ入力される。ここまでは図１に示した他の実施形態における動作と全く同様である。ＭＰＥＧ分離回路５０９ではトランスポートストリーム形式で送られてきたＥＣＭ情報及びＥＭＭ情報を検出し、それぞれ端子５６９、５６８を通して鍵情報分離回路５０５に送る。鍵情報分離回路５０５は送られてきたＥＣＭ情報より暗号化された第１の鍵データを抽出し、端子５５６を介して第１の鍵復号回路５０７へ送出する。また鍵情報分離回路５０５はＭＰＥＧ分離回路５０９より送られてきたＥＭＭ情報より暗号化された第２の鍵データを抽出し、端子５５７を介して第２の鍵復号回路５０６へ送出する。郵送などの配送手段によって、伝送路７００を経由して入手したＩＣカード等の情報記憶媒体５１３から得られた第３の鍵データを端子５５８を介して第2の鍵復号回路５０６に供給する。第2の鍵復号回路５０６では第３の鍵データによって暗号化された第２の鍵データを復号することによって、第２の鍵データが得られる。この第２の鍵データは一旦第２の鍵データ記憶手段５２０に蓄えられた後端子５７３を介して第1の鍵復号回路５０７へ送られる。第1の鍵復号回路５０７では第２の鍵データ記憶手段５２０より送られた第２の鍵データを用いて暗号化された第１の鍵データを復号して第１の鍵データが得られる。復号された第１の鍵データは第１の鍵データ記憶手段５２１に記憶された後、端子５７２を介してコンテンツデスクランブル回路５０８に送られる。以後、必要な場合は第１の鍵データ記憶手段５２１に記憶された第１の鍵データ５７２がコンテンツデスクランブル回路５０８に送られることになる。コンテンツデスクランブル回路５０８では、第１の鍵データ記憶手段５２１より送られた第１の鍵データを用いて、暗号化され且つ誤り訂正されたデジタルデータを復号して、ＭＰＥＧ2トランスポートストリーム形式のデスクランブルデジタルデータに戻され、ＭＰＥＧ多重分離回路５０９で圧縮映像データ５６２と圧縮オーディオデータ５６３に分離されてＭＰＥＧビデオデコーダ５１０とオーディオデコーダ５１２に入力される。

【００４１】圧縮映像データはＭＰＥＧビデオデコーダ５１０によって映像データ５６４に変換され、ＮＴＳＣビデオエンコーダ５１１によってＮＴＳＣビデオ信号に変換される。圧縮オーディオデータはオーディオデコーダ５１２によってアナログオーディオ信号に変換される。ＮＴＳＣビデオ信号とアナログオーディオ信号はそれぞれ端子５６５，５６６を介して映像音声表示器６００に入力されて、映像音声表示器６００で表示された映像と音声などの情報を視聴者に提供できる。また、選局要求に従って第１の鍵データ記憶手段５２１より送られた第１の鍵データを使用してコンテンツデスクランブル回路５０８でデスクランブルできない場合には、改めてＭＰＥＧ分離回路５０９よりＥＣＭ情報を抽出し鍵情報分離回路５０５を通して第１の鍵復号回路５０７により暗号化された第１の鍵データを復号し、共に第１の鍵データ記憶手段５２１の内容を更新すると共に、第１の鍵データをコンテンツデスクランブル回路５０８に送信することでコンテンツデスクランブル回路５０８においてデスクランブルが可能となる。

【００４２】図５は本発明によるケーブルテレビの限定受信システム並びのその送信装置及びその受信装置のさらに他の実施例を示すブロック図である。図５において、１０２はＥＣＭ情報を記憶して設定された頻度でトランスポートストリーム形式のデジタルデータとして時分割多重する時分割多重回路でありＥＭＭ情報の記憶手段は含んでいない。その他は図１と同じである。ケーブルテレビの送信側で限定受信システムにおける負荷の低減および違法受信対策のためＥＭＭ情報の送出頻度を低くする場合が考えられる。例えば、ＥＭＭ情報の更新を１日に１回行うような場合には、ＥＭＭ情報を常に送出すると伝送効率が下がる。よって、ＥＭＭ情報の更新頻度が少ない場合にはＥＭＭ情報を常時送出する必要はない。この場合時分割多重回路１０２におけるＥＭＭ記憶

回路は必要ではなくなる。むしろ受信側端末装置５００におけるＥＭＭ記憶手段５１５において低い頻度で送信されるＥＭＭ情報を記憶することにより、短時間でのスクランブルの解除が可能となる。なお、時分割多重回路１０２にＥＭＭ記憶手段を設けな場合、ＥＭＭ情報は外部装置、例えばパソコンを通して時分割多重回路１０２に入力されるため、ＥＭＭ情報の送出頻度はこの外部装置の能力によって左右される。また、本実施例では受信側端末装置５００の動作は図１に示した実施例と全く同様である。

【００４３】図６は本発明によるケーブルテレビの限定受信システム並びのその送信装置及びその受信装置のさらに他の実施例を示すブロック図である。図６において、１０２はＥＣＭ情報を記憶して設定された頻度でトランスポートストリーム形式のデジタルデータとして時分割多重する時分割多重回路でありＥＭＭ情報の記憶手段は含んでいない。５２０は第２の鍵データ記憶手段である。記憶された第２の鍵データは第２の鍵データ記憶手段５２０の端子５７３に取り出される。その他図１と同じ機能を有するブロックには同一の符号付けた。

【００４４】受信側端末装置５００では、周波数多重されて伝送された６４ＱＡＭデジタル被変調波信号をＣＡＴＶ伝送路４００から受け、周波数多重信号分離回路５０１で制御用マイコン５０２からの制御信号に応じて選局される。この選局された６４ＱＡＭ被変調波信号は６４ＱＡＭ復調回路５０３に入力される。６４ＱＡＭ復調回路５０３で６４ＱＡＭ被変調波信号は６４ＱＡＭ復調デジタルデータに復調され、誤り訂正回路５０４により伝送路で生じたデータの誤りが訂正される。誤り訂正されたデジタルデータはコンテンツデスクランブル回路５０８に入力される。誤り訂正回路５０４では、インターリーブ処理やエネルギー拡散処理されたデータの復号も行なわれる。第１の鍵データが復号されるまではコンテンツデスクランブル回路５０８においてデスクランブルは実行されず誤り訂正後デジタルデータはそのままＭＰＥＧ分離回路５０９へ入力される。ＭＰＥＧ分離回路５０９ではトランスポートストリーム形式で送られてきたＥＣＭ情報及びＥＭＭ情報を検出し、ＥＣＭ情報をＥＣＭ記憶手段５１４へ送付し、ＥＭＭ情報を鍵情報分離回路５０５に送る。鍵情報分離回路５０５はＥＣＭ記憶手段５１４より送られてきた記憶されたＥＣＭ情報より暗号化された第１の鍵データを抽出し、端子５５６を介して第１の鍵復号回路５０７へ送出する。また鍵情報分離回路５０５はＭＰＥＧ分離回路５０９より送られてきたＥＭＭ情報より暗号化された第２の鍵データを抽出し、端子５５７を介して第２の鍵復号回路５０６へ送出する。

【００４５】第2の鍵復号回路５０６では、郵送などの配送手段により伝送路７００を経由して入手したＩＣカード等の情報記憶媒体５１３からの第３の鍵データによって、暗号化された第２の鍵データを復号して第２の鍵復号回路５０６の出力端子５５９に第２の鍵データが得られる。この第２の鍵データは一旦第２の鍵データ記憶手段５２０に蓄えられた後、第1の鍵復号回路５０７へ送られる。第1の鍵復号回路５０７では第２の鍵データ記憶手段５２０より送られた第２の鍵データを用いて暗号化された第１の鍵データを復号して、その出力端子５６０に第１の鍵データを得る。復号された第１の鍵データはコンテンツデスクランブル回路５０８に送られる。コンテンツデスクランブル回路５０８では、第1の鍵復号回路５０７より送られた第１の鍵データを用いて、暗号化されており、且つ誤り訂正されたデジタルデータを復号して、ＭＰＥＧ2トランスポートストリーム形式のデスクランブルデジタルデータに戻され、ＭＰＥＧ多重分離回路５０９で圧縮映像データと圧縮オーディオデータに分離され、それぞれＭＰＥＧビデオデコーダ５１０とオーディオデコーダ５１２に入力される。圧縮映像データはＭＰＥＧビデオデコーダ５１０によって映像データに変換され、ＮＴＳＣビデオエンコーダ５１１によってＮＴＳＣビデオ信号に変換される。圧縮オーディオデータはオーディオデコーダ５１２によってアナログオーディオ信号に変換される。ＮＴＳＣビデオ信号とアナログオーディオ信号は映像音声表示器６００に入力されて、映像音声表示器６００で表示された映像と音声などの情報を視聴者に提供できる。また、選局要求に従って前記ＥＣＭ記憶手段５１４に記憶されているＥＣＭ情報より第１の鍵復号回路５０７によって復号された第１の鍵データを使用してコンテンツデスクランブル回路５０８でデスクランブルできない場合には改めてＭＰＥＧ分離回路５０９よりＥＣＭ情報を抽出し、ＥＣＭ記憶手段５１４の記憶内容を更新すると共に鍵情報分離回路５０５を通して第１の鍵復号回路５０７により暗号化された第１の鍵データを復号することでコンテンツデスクランブル回路５０８においてデスクランブルが可能となる。

【００４６】

【発明の効果】本発明によれば、デジタル方式の限定受信システムを成立させる情報であるＥＣＭ情報とＥＭＭ情報を記憶する手段を送信側と受信側双方に設けることによって、システム負荷や盗聴に対するセキュリティ上の問題に大きく関係するＥＣＭ情報およびＥＭＭ情報の送出頻度をシステムの運営に合わせて設定することができ、且つ短時間でのチャンネル選択（スクランブルの解除）を可能にすることが出来る。また、本発明によれば、受信装置にＥＣＭ情報を記憶するＥＣＭ記憶手段を設けているので、ＥＣＭ情報を利用して前記第１の鍵データを抽出でき、選局から映像や音声がスクランブルを解かれて出力するまでのいわゆる選局動作を短くすることができる。また、ＥＣＭ情報が変更された場合など、このＥＣＭ記憶手段に記憶したＥＣＭ情報を利用してデスクランブル処理ができない場合には、復調手段から新

しくＥＣＭ情報を抽出し、記憶されているＥＣＭ情報を更新して利用できる。

【図面の簡単な説明】

【図１】本発明によるケーブルテレビの限定受信システム並びのその送信装置及びその受信装置の一実施例を示すブロック図である。

【図２】本発明の実施例を説明のためのＭＰＥＧ2トランスポートストリーム形式の信号構成を示す概念図である。

【図３】本発明の実施例を説明するためのＭＰＥＧ2トランスポートストリーム形式のパケットヘッダの信号構成を示す概念図である。

【図４】本発明によるケーブルテレビの限定受信システム並びのその送信装置及びその受信装置の他の実施例を示すブロック図である。

【図５】本発明によるケーブルテレビの限定受信システム並びのその送信装置及びその受信装置のさらに他の実*

*施例を示すブロック図である。

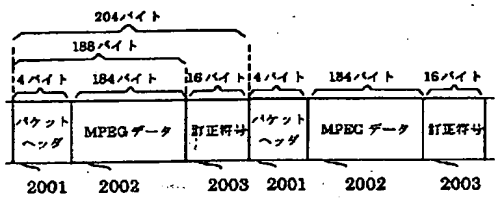
【図６】本発明によるケーブルテレビの限定受信システム並びのその送信装置及びその受信装置のさらに他の実施例を示すブロック図である。

【符号の説明】

１００…送信側暗号化変調装置、２００…送信側映像信号源装置、３００…送信側鍵等管理装置、４００…ＣＡＴＶ伝送路、５００…受信側端末装置、６００…受信側ＴＶ受像機、１０１…暗号化装置、１０２…時分割多重回路、１２１…ＥＣＭ記憶回路、１２２…ＥＭＭ記憶回路、１１１…映像音声多重化及びコンテンツスクランブル回路、１１２…スクランブル制御装置、１１３…限定受信制御装置、５０３…６４ＱＡＭ復調回路、５０６…第2の鍵復号回路、５０７…第1の鍵復号回路、５０８…コンテンツデスクランブル回路、５１４…ＥＣＭ記憶手段、５１５…ＥＭＭ記憶手段。

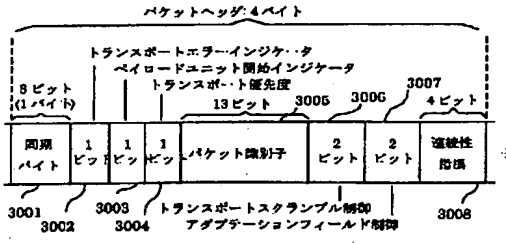
【図２】

図２



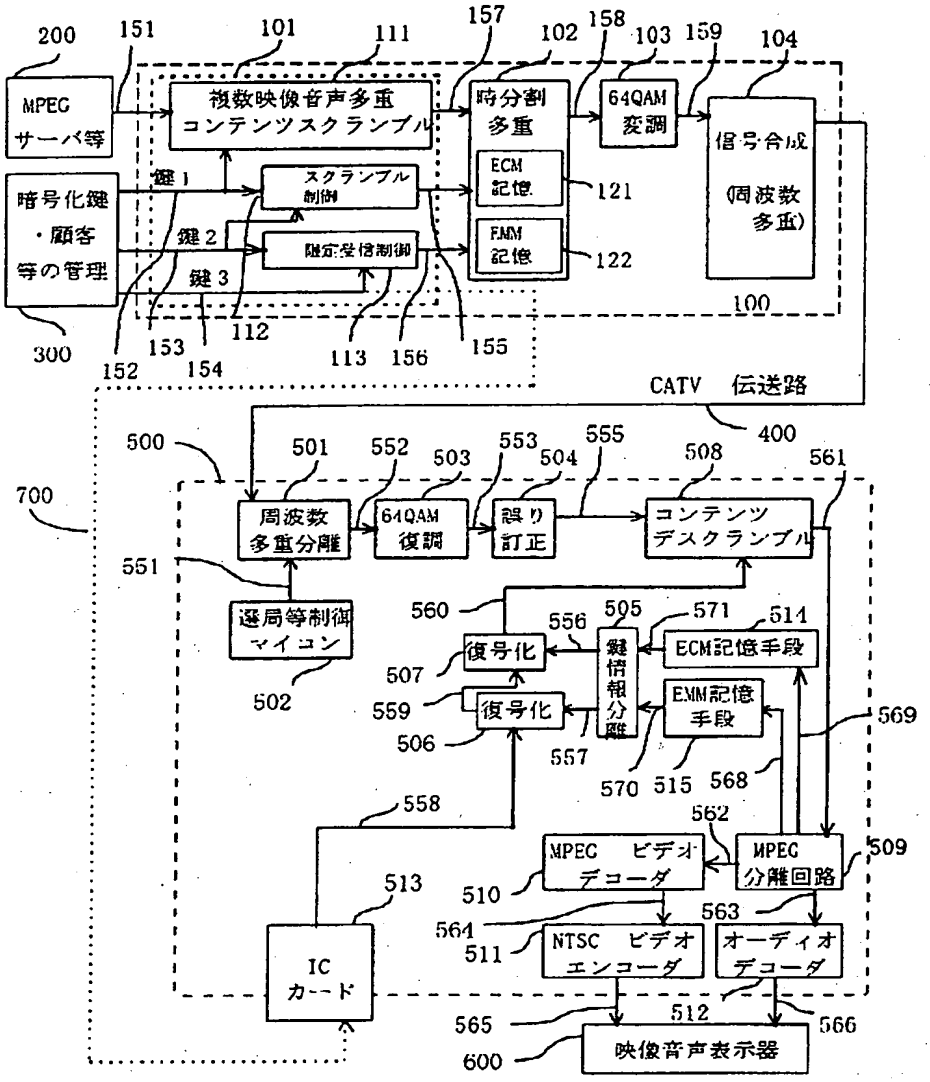
【図３】

図３



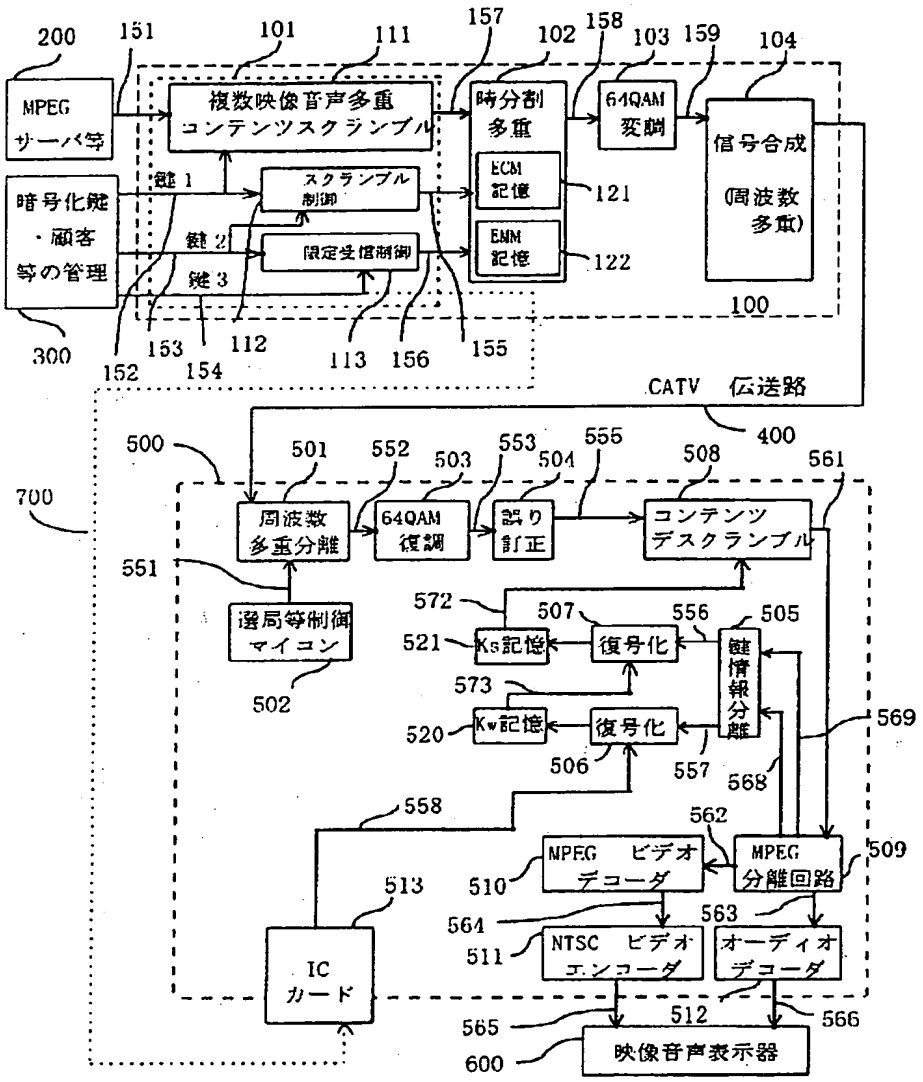
【図１】

図 1



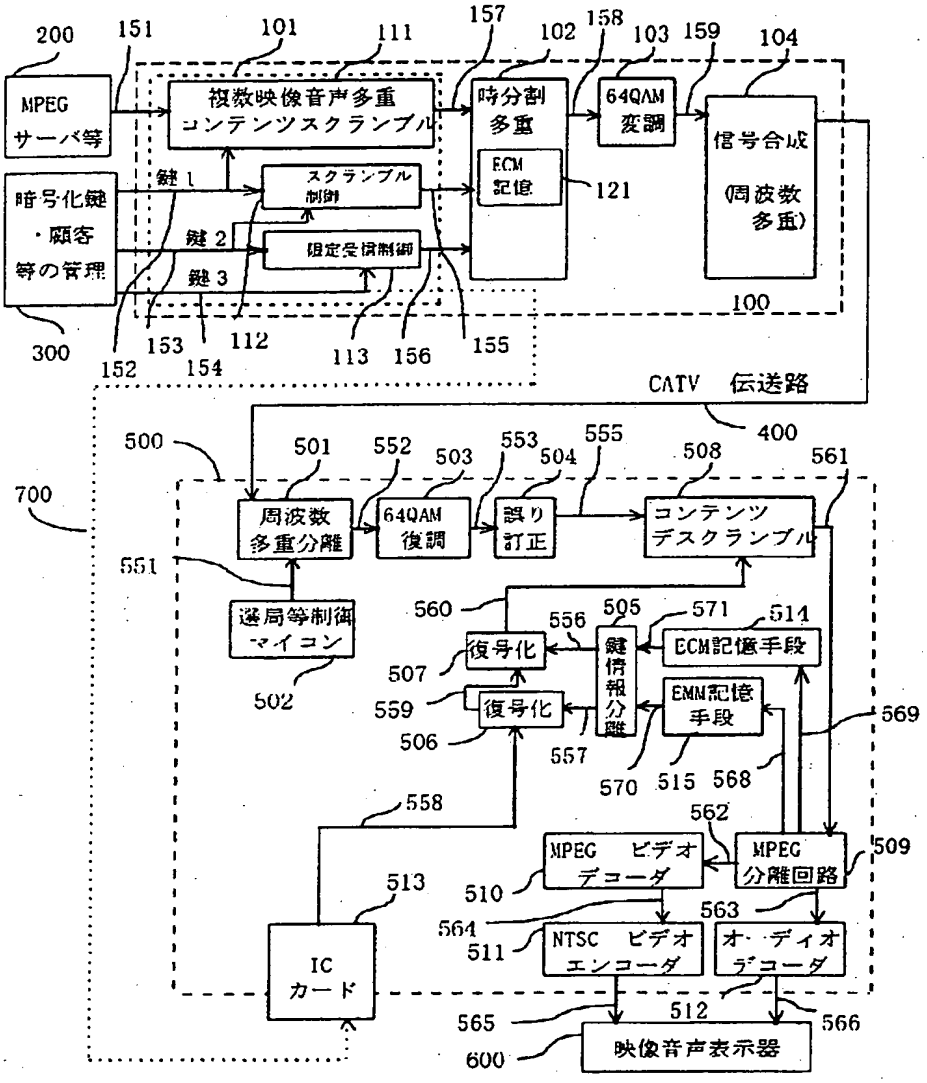
【図４】

図 4



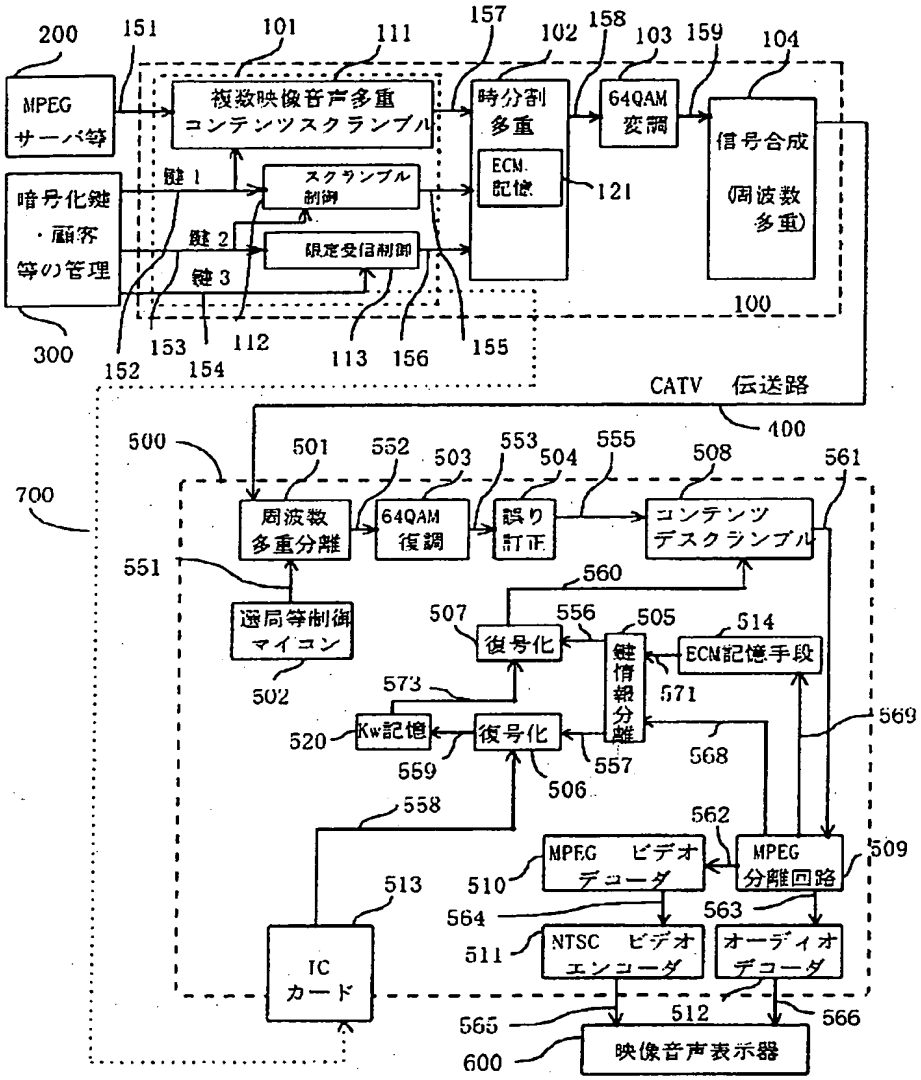
【図５】

図５



【図６】

図６



フロントページの続き

(51) Int.Cl.[7]	識別記号	F I	テーマコード（参考）
		H04L 9/00	601E

(72)発明者 西田 正巳
神奈川県横浜市戸塚区吉田町292番地 株式会社日立製作所ＡＶ事業部内

Ｆターム（参考） 5C064 BA01 BB02 BB05 BC16 BC17 BC20 BC22 BD07 BD08 CA18 CB01 CC01
5J104 AA16 BA03 EA18 EA22 NA02 NA35 PA06